

# **Fight the Network**

***An Enterprise Operational Framework for Global Unit of  
Employment (x) - UEx, Unit of Employment (y) - UEy, and  
Brigade Combat Team - BCT Joint and Expeditionary  
Network Operations***

***Army Chief Information Officer/G-6 White Paper  
September 2004***

## ARMY CHIEF INFORMATION OFFICER (CIO)/G-6 INTRODUCTION

“We must change the paradigm in which we talk and think about the network; we must “fight” rather than “manage” the network and operators must see themselves as engaged at all times, ensuring the health and operation of this critical weapons system.”

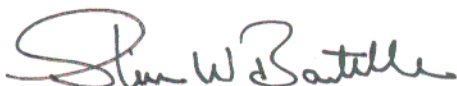
– *Serving a Nation at War: A Campaign Quality Army with Joint and Expeditionary Capabilities*

The Network enables joint and expeditionary battle command. The Network is, at its very core, more than simply pushing electrons around the globe and throughout the battlespace. It is about enabling the leaders of the joint and expeditionary force with the capability to command and control large maneuver formations, sustain the force with minimal forward presence, and achieve broad political-military objectives across the full spectrum of operations.

For this vision to be a reality, the Network must be a single integrated entity and not a collection of functional stovepipes. It must be pervasive throughout the battlespace and must touch every entity to include the individual soldier. Although the Army fights by echelon, the pervasive nature and global interdependency of the Network, unbounded by space and time, requires it be fought with a different paradigm. Furthermore, this complex, global, joint entity requires operations and cyber defenses that can leverage strategic and national capabilities.

The necessity for unity of effort extends vertically and horizontally beyond traditional organizational boundaries. The Network must be fought as an enterprise by a Network commander throughout all echelons. Units and soldiers must be trained and ready to maneuver network assets throughout the battlespace in real-time to support the joint force commander. Network commanders must be accountable for the entire infostructure and manage all networks at their respective echelon. Network formations must provide scaleable, joint, interoperable capabilities that are operated, defended, trained, equipped, and fought under global standards and configurations.

The “Fight the Network” paradigm presented in this white paper will enable the Signal Regiment to guide signal transformation and doctrine development. Modern warfare is immensely complex and requires interoperability, synchronization, and synergy of all systems to achieve full spectrum dominance. Never before has the Signal Regiment been as critical to the success of our Army.



STEVEN W. BOUTELLE

Lieutenant General, GS

Chief Information Officer/G-6

## PURPOSE

“The lesson of this war is that effectiveness in combat will depend heavily on jointness – that is, the ability of different branches of our Military to communicate and coordinate efforts across the battlefield.” Secretary of Defense Donald Rumsfeld

- *Foreign Affairs* May/June 2002

Twenty-First Century warfare mandates information age capabilities to support the battle command requirements of the joint force commander. The joint force commander and subordinate elements to the lowest levels must be able to “see first, understand first, act first, and finish decisively.” This is the essence of Army transformation.

The Network is essential for enabling the Army to rapidly transform and execute full spectrum joint and expeditionary campaign quality operations. Expeditionary operations require the Network to be uniform, pervasive, and centrally managed with common standards throughout all echelons to preclude interoperability failures.

This white paper analyzes the strategic environment; Army initiatives; the command, control, communications, and computer (C4) operational environment; and the emerging Network and Network imperatives. This analysis provides a capability-based lens to draw conclusions about how to fight the Network. These conclusions build the foundation for the Signal Regiment to guide signal transformation and Doctrine, Organization, Training, Materiel, Leadership Personnel, and Facilities (DOTML-PF).

## STRATEGIC ENVIRONMENT

In 2001, the Department of Defense (DoD) introduced the concept of Net-Centric Operations and Warfare (NCW). NCW is an information superiority-enabled concept of operations (CONOPS) that generates increased combat power by networking sensors, decision makers, and shooters to achieve situational awareness, increased speed of command, higher tempo of operations, increased survivability, and a degree of self-synchronization. NCW will allow the joint force to deploy anywhere, at anytime, to achieve national political-military objectives across the full spectrum of operations. This includes the capability to function effectively in an informed manner in a range of operating environments from austere to built-up areas. The infostructure that supports commanders and their sustaining bases must be equally responsive, tailorable, scalable, and robust. As the Army transforms, the Network—battle command, communications, and information capabilities (including command & control, intelligence, surveillance, reconnaissance, and combat service support)—must be transformed accordingly.

“...net-centric operations environment ~ a global information grid (GIG) that provides an end-to-end set of information services, associated processes and people to manage and provide the right information to the right user at the right time with appropriate protection across all DoD war fighting, intelligence and business domains.”

- *Joint CONOPS for GIG NetOps*, May 04



## Fight the Network

The GIG is a massively networked environment of numerous complex interconnections with dynamic capabilities asynchronously deployed. The Defense Information Systems Agency (DISA) is responsible for the end-to-end administration and integration of the Defense Information Systems Network (DISN) and the GIG. However, the majority of the GIG is comprised of networks operated by each Service (Figure 1).

### JOINT ENTERPRISE – BUY-IN BY ALL SERVICES

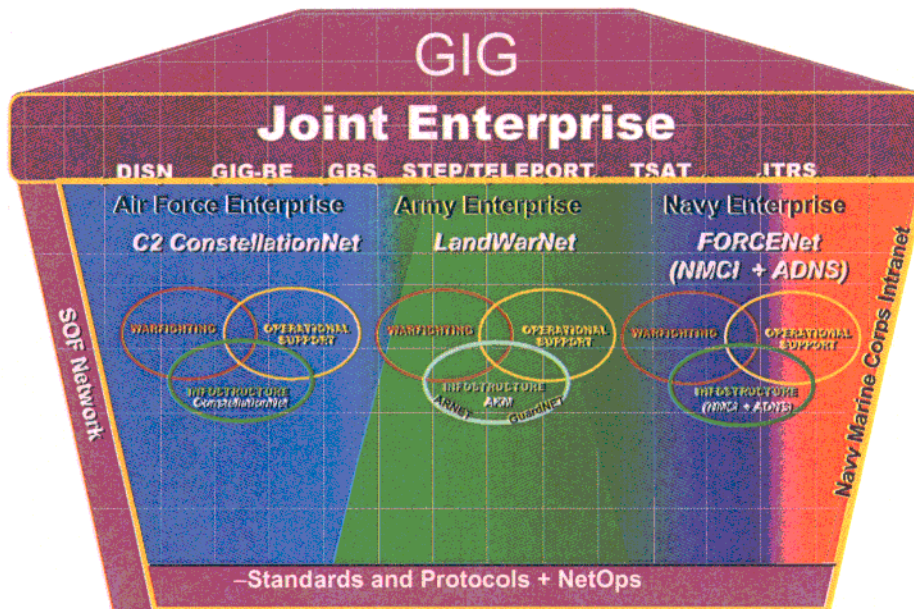


Figure 1

These networks were developed largely in isolation and have evolved into an integrated system, yet seams remain that must be eliminated for the full power of the information age to be realized. This essential integration includes the complete sharing of joint and military service data. The soldier on the ground should have the capability to access and direct fire support just as the aircraft flying overhead should have the latest common operational picture of the battlespace.

Of growing importance is the integration of DoD networks into commercial, coalition, and other governmental agencies' networks. The DoD cannot and must not expect to operate in a purely military environment. The norm will be a diverse battlespace that will include a variety of different entities with varying degrees of information requirements. The demand for shared voice and data capabilities requires common software, hardware, standards, protocols, and applications. The DoD has moved to Internet Protocol (IP) services as the protocol of choice, and the Army is quickly migrating to an IP-based architecture.

The GIG is continuously evolving. The Army's Land Warrior Network (LandWarNet) is part of the larger GIG and comprises all Army operational networks (National Guard, Army Reserve, and Active Army) that are integrated, interoperable, and nested within the joint

## Fight the Network

enterprise. As the overall GIG matures, the LandWarNet will mature in a parallel and complementary manner and will be operated within joint operational constructs.

The DoD construct for the operation and defense of the GIG is Network Operations (NetOps). The goal of NetOps is to provide assured net-centric services across strategic, operational, and tactical boundaries in support of the DoD's full spectrum of warfighting, intelligence and business missions. The DoD has assigned the global NetOps mission to a combatant commander.

“Commander, STRATCOM, is the supported commander for Global NetOps, and has the authority to direct Combatant Commanders, Services and Agencies to take action to ensure the availability and integrity of the GIG.”

- Joint CONOPS for GIG NetOps, May 04

To provide unity of effort to Commander, United States Strategic Command (STRATCOM), the DoD Joint CONOPS for NETOPS directs that combatant command (COCOM), and military service NetOps capabilities for operating and defending the GIG be under centralized management and control, as in the Army today. To support NCW and information superiority, the Army has taken deliberate actions to mandate an enterprise approach to operate, manage, and defend the Network. This enterprise level approach is not unique to the DoD. The most successful industry information technology service providers centrally manage and control their networks. The U.S. Air Force, U.S. Navy, and U.S. Marine Corps have also started enterprise transformation initiatives and are sharing best practices and lessons learned.

## ARMY INITIATIVES

Transformation of the Army's C4 structure and mission roles began in 2001 with the Headquarters, Department of the Army Realignment Task Force (RTF) under the Deputy Under Secretary of the Army. The RTF recognized the importance of a structured and enterprise approach to C4 missions across the Army and directed establishment of an Army G-6, dual hatted as the Army CIO (GO #3, dated 9 July 2002). The G-6 provides strategic direction and the oversight for signal operations, network and communications security, force structure, and equipping and employment of signal forces. The CIO serves as principle advisor to the Chief of Staff (CSA) for all information management functions pursuant to Public Law 10 U.S.C. Section 2223 and Public Law 104-106.

Army General Order #5, dated 11 July 2002, furthered the transformation of the Army's C4 structure by establishing Network Enterprise Technology Command/9<sup>th</sup> Army Signal Command (NETCOM), a direct reporting unit to the CIO/G-6, as the single authority to operate, manage, and defend the Army infostructure at the enterprise level. The mission of NETCOM is to deliver seamless enterprise level C4 and information technology, common user services, and signal warfighting forces in support of the Army, its Army Service Component Commanders (ASCCs), and the combatant commanders. To ensure adherence to joint and enterprise standards, NETCOM has technical control and configuration management authority for the LandWarNet. Additionally, to assure effective integration and global mission execution,



## Fight the Network

NETCOM is assigned the responsibility for force structure, resource management, personnel management, training, commercial off-the-shelf (COTS) technology sustainment, and equipping for the Army's worldwide strategic and theater tactical signal forces. The U.S. Army Signal Center, a component of the Training and Doctrine Command, complements this direction from the CIO/G-6 with operational execution under NETCOM by providing DOTML-PF products that encompass the joint perspective.

To posture the Army to support joint NetOps mandates, Deputy Secretary of Defense (DEPSECDEF) directed (May 2003) that the U.S. Army Network Operations and Security Center (ANOSC), responsible for the Army NetOps situational awareness and reporting, be co-located and integrated with the Army Computer Emergency Response Team (ACERT). This integration created a centralized team of experts to spearhead the defense of the Army's networks, which is executed by forces under the operational control (OPCON) of the ASCC.

The benefits of these transformational directives are apparent today. All components (Army Reserve, National Guard, and Active Army) are teaming to create a seamless interoperable enterprise. Active and Reserve component NetOps forces are being restructured and modernized to deliver modular, tailored C4 capabilities. The Army has published a joint compliant Army NetOps architecture that defines the framework for ensuring the delivery of C4 capabilities. Enterprise contracts and licenses are reducing costs while creating a more secure, sustainable, interoperable, and robust infostructure. Army Knowledge Online (AKO) is the largest portal within the DoD and is enabling the transformation of key processes.

This enterprise focus has positioned the Army to operate and defend the Network as a warfighting platform and enabled unprecedented levels of support to Operation Enduring Freedom/Operation Iraqi Freedom (OEF/OIF) operations. These initial enterprise initiatives are enabling the Signal Regiment to rapidly embrace and respond to the transformation challenge of becoming a "campaign quality Army with joint and expeditionary capabilities." To guide efforts to transform the force, the Army established 17 focus areas. All of these focus areas deal with some component of developing information age capabilities for the Army's current and future force. Of the 17 focus areas, the following eight frame the direction and capabilities of the Network:

- The Network—Leverage and enable interdependent network-centric warfare.
- Modularity—Create modular, capabilities-based unit designs.
- Joint and Expeditionary Capability—Retain our campaign qualities while developing joint and expeditionary capability.
- Current to Future Force—As quickly as possible integrate information age technologies into the current force, while bringing key programs such as Warfighter Information Network-Tactical (WIN-T) and Joint Tactical Radio System (JTRS) to the field as rapidly as possible.
- Installations as Flagships—Ensure that the posts, camps, and installations support the deployed force with information age capabilities. This includes upgrading the existing infrastructure as well as developing standard level of service templates for future Army installations.
- Actionable Intelligence—Ensure commanders have access to timely intelligence (information), which is essential to an information age force.

## Fight the Network

- Focused Logistics—Ensure flow of logistics information, the key ingredient for successful support for this focus area.
- Soldier—Ensure flexible, adaptive, and competent soldiers.

Achieving a joint and expeditionary mindset will require a revolutionary shift in how the Army operates, resulting in major redesign and restructuring at all echelons throughout the active and reserve components. While a key enabler of transformation, the Network itself will experience revolutionary change.

## OPERATIONAL C4 ENVIRONMENT

The intent of the transformed Army is to create a modular force whose capabilities can be tailored to respond to regional combatant commanders' (RCCs') needs, better employ joint capabilities, facilitate force packaging and rapid deployment, and fight as an autonomous unit (linked by the Network) in a nonlinear, noncontiguous battlespace. This new paradigm demands the creation of modular formations that are not tied to a division base that can be simultaneously deployed from multiple power projection platforms and are tailorable for full spectrum operations.

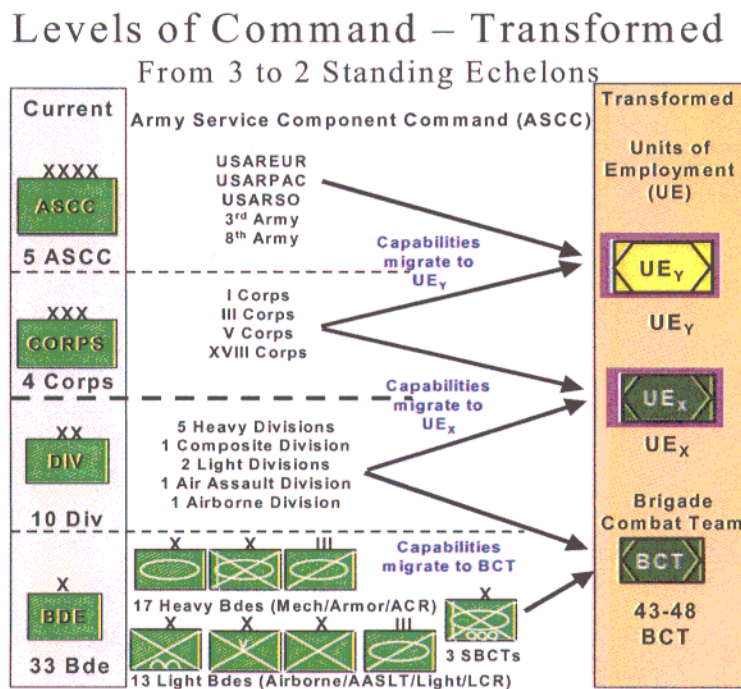


Figure 2

The precise force structure and force/equipment mix is still being developed, but the expected echelons and capabilities of the transformed Army and its Unit of Employment y (UEy)/Unit of Employment x (UEx)/Brigade Combat Team (BCT) force mix are shown in Figure 2. The effect of the altered echelons is to eliminate a level of command. The battle command structure

## Fight the Network

will also be more streamlined with fewer layers between the combatant commander and the BCT in the fight. The strategic environment, coupled with the demands of network-centric expeditionary operations, significantly increases reliance on the Network. The Network should be immediately available to the joint force commander and subordinate elements upon arrival in theater. Each UEx and BCT must be prepared to fight upon arrival. Therefore, they must be trained and interoperable with any UEy, with another UEx or BCT, and with the joint/combined forces throughout all phases of deployment. Units must have access to real-time information in transit and immediately upon arrival. The UEx must be able to integrate and synchronize multiple BCTs. The UEy must be able to receive, coordinate, and employ a varying mix of UEx and BCTs, interact with other UEys around the globe, and be tailorable to support a Joint Task Force (JTF)/Coalition Forces Land Component Command (CFLCC) headquarters element.

In support of the complex and dynamic environment, the Network will be critical in providing reliable and relevant information for situational awareness, joint command, joint fires, joint lift, joint logistics, targeting, intelligence, and mission planning. The requirement for comprehensive Network services at all echelons has blurred the distinctions between coalition, joint, strategic, and tactical networks. “Plug and Play” across the enterprise can no longer be loosely supported; the Network must be accessible and maneuvered across all operational phases (Figure 3).

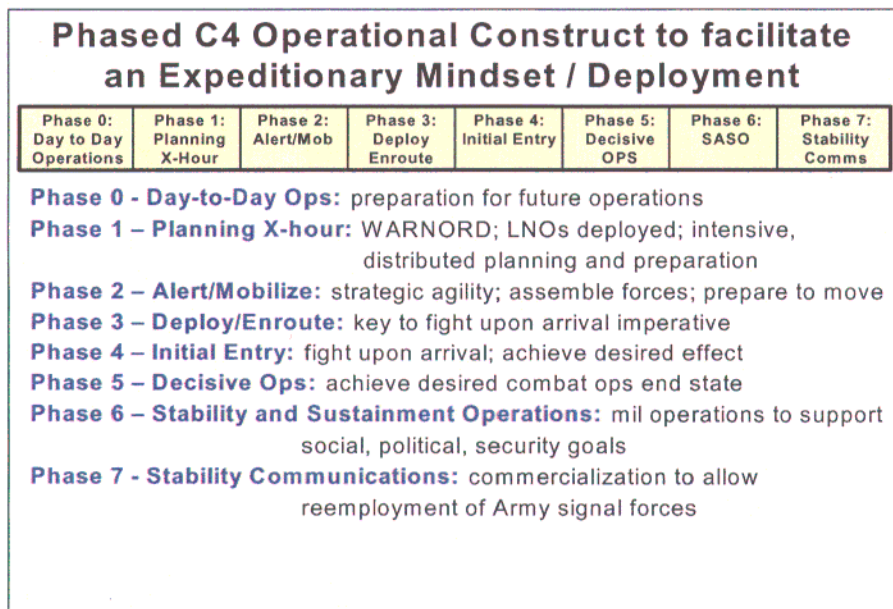


Figure 3

Each phase represents major operational transitions and changes that the critical organizations and staffs must communicate and coordinate. Commanders will have a variety of high-capacity battle command systems available. Commanders and staff do not necessarily need to know how the service is being provided, but rather that the service will be available on demand. Consequently, the Network must know that the information exists and how to access it. Thus, priority of effort for the Network will continually change—the phases are sequential for any one



element's deployment and employment, but the Network will constantly and simultaneously execute multiple priorities around the globe. For example, during Phase 2, priority of C4 effort is on the UEy, UEx, and BCT in geographically disparate home station locations, but in Phase 3 priority shifts to elements enroute, sea ports of embarkation (SPOE), and aerial ports of embarkation (APOE). A task force with simultaneous deployments and employments can simultaneously span multiple phases and theaters.

Unlike the past, commanders and soldiers must have a full suite of Network capabilities throughout all phases—in garrison, Home Station Operation Centers (HSOC), enroute and when deployed. To meet the demands of the strategic and operational environment, the Army is taking deliberate action to enable Network transformation and provide responsive support to the warfighter around the globe. These transformed Network capabilities will pervade all aspects of the battlespace and will accelerate operational and cultural changes throughout the military services.

## THE NETWORK

Like the Army, the Network is echeloned and interdependent:

- Coalition, multinational, interagency, and commercial networks exist throughout the battlespace but must be fully integrated to fight the Network. The DoD's dependence on commercial networks and competing commercial priorities adds additional complexity to planning and execution. These commercial networks may include the communications infrastructure of hostile or occupied territories. The challenges associated with network security in this "mixed" network environment cannot be ignored.

- Joint access to the GIG and its services are provided through standard tactical entry points (STEPS), teleports, and other points of presence (POPs) located in all theaters and coordinated by the UEy for the Army. Joint doctrine and policy must govern operations due to their global interdependence. For example, U.S. Central Command (CENTCOM) reach back occurs through C4 facilities located in U.S. Pacific Command (PACOM), U.S. European Command (EUCOM), and continental United States (CONUS); network disruption in Europe can affect Blue Force Tracking for Southwest Asia. The Army, along with the other Services and DISA must work in concert to ensure that only the most modern capabilities and systems are fielded to these sites, while

*The Joint Fires Officer (JFO) is monitoring a screen; on the left side of the screen is a list of all the radars and sensors from all military services in the JTF that are available. On the bottom of the screen are all of the weapon systems that are available for fires missions. Linking sensor to shooter, the JFO makes a selection to prosecute the target. As soon as the mission is complete, the assets available for the next mission are displayed. The target is hit, and the JFO calls up the Battle Damage Assessment (BDA) screen, looks at assets available for BDA, and posts the BDA information to the network so all "fires" officers have the same situational awareness.*

## Fight the Network

maintaining backwards compatibility for servicing those units that have not been fully modernized.

- Theater networks are an extension of the GIG and support operations and strategic functions for the RCC and the Army's UEy. The UEy Network operates continuously and extends horizontally and vertically to enable simultaneous full spectrum operations while sustaining Army business lines and reach back to installations, Power Projection Platforms (PPPs), and Power Support Platforms (PSPs). It is at the UEy level that critical theater resources (e.g., spectrum, frequency, satellite access) are allocated and synchronized with the RCC requirements. The UEy Network, through fixed and deployable formations, delivers DISN services and the Army capabilities that comprise the theater GIG. Additionally, the UEy Network supports COCOM and host nation unique requirements. Besides coordinating daily theater operations and the theater signal battle, UEy Network forces may augment UEx and BCT operations.
- The UEx and BCT rely on the Network for battle command, intelligence, and combat service support (CSS) operations. They must leverage internal, strategic, and national capabilities and the UEy to orchestrate the theater Network battle. UEx and BCT will deploy into theaters from multiple force projection platforms. OIF lessons learned highlighted initial operational risk from shortfalls caused by lack of interoperability standards. Therefore, this complex environment demands full connectivity, complete synchronization, and consistent worldwide standards to allow immediate access to the fight. UEx and BCT will dynamically maneuver forces and Network capabilities within the enterprise. The integration of Network capabilities across all echelons (BCT to BCT, BCT to UEx, UEx to UEy, etc.) will require total synchronization across all NetOps disciplines.

The Network is joint focused and is based on a mix of military and commercial systems that capitalize on new and emerging technologies to provide enhanced capabilities to commanders and staffs at echelons far below echelons that had these capabilities in the past. The Network must be a single secure grid providing:

- Seamless end-to-end capabilities for:
  - National security, DoD, and intelligence community requirements from peacetime business support through all levels of conflict.
  - Strategic, operational, tactical, base, post, camp, and station levels.
  - Warfighting and support users.
- Information fusion capabilities for:
  - Joint high capacity netted operations.
  - Linking state-of-the-art weapons and intelligence, surveillance, and reconnaissance (ISR) systems.
  - U.S. Government interagency information sharing capability.
  - Tactical and functional fusion.
- "Plug-and-Play" interoperability and connectivity between U.S. and coalition users.



## Fight the Network

- Information and bandwidth on demand.
- Defense in depth against all threats.

The Network is more than just hardware and software; the ability to use the Network to fight in the 21<sup>st</sup> Century battlespace is directly linked to the human factors associated with battle command. Joint force commanders must not only understand and believe the information that is coming through the Network; the Network must enable the sharing of knowledge so that commanders can take decisive action.

An important aspect of the Network will be the development of the soldier C4 systems. The inclusion of the soldier as part of the Network is a fundamental conceptual element in Army transformation. While it is a concept that might appear foreign, the 3,500 “collectors” in a maneuver BCT are likely to provide the most reliable “ground truth” for the commander.

The life cycle of Network technology is dramatically shorter than other functional areas—on the order of months versus years. This compressed life cycle and greater reliance on commercial-off-the-shelf (COTS) equipment continuously introduce network vulnerabilities and enable our opponents to rapidly find new ways to threaten and exploit our Network. As the number of entities within the Network grows, this problem will become more acute. Technologies that used to take months to exploit now take days or even hours. To mitigate these life cycle challenges, Network operators and defenders require current and relevant tools, technical skills, standards, and authorities across all Network echelons.

The people who operate, manage, and defend the Network are a diverse mix, consisting of soldiers, government civilians, and contractors. They are equally as important as the Network hardware and software. The DoD’s strong reliance on commercial partnerships for manpower cannot be ignored and influences leader development, training, force design, and Network processes.

Network capabilities are not without a human cost and will require significant individual and collective training to master. The Network will affect what tasks we train on and how we train. Learning will be a lifelong process, and the military services will work together more closely in the procurement of systems and training of their leaders, soldiers and civilians to fight in a ubiquitous Network environment.

*A wounded soldier is taken to a battalion aid station. The soldier has an injured hand and needs surgery within 96 hours. Hand surgeons are rare, especially on the battlefield. An enterprising Army Specialist (SPC) at the aid station gets on the computer, checks the Joint Surgeons Directory, and locates a Navy hand surgeon in Naples, Italy. The SPC calls up the surgeon’s schedule and sees that the doctor has an opening in two days and books the surgery, writes a description of the patient’s injury, and sends the medical records to the Naples hospital. The wounded soldier needs transportation, so the SPC goes to the applications web site, finds the transportation application needed, and then books transportation from the aid station to the Naples hospital. Knowing that the soldier is not likely to return to the unit because recuperation time will be six to eight months, the SPC goes to the application web site and requisitions a replacement.*

Innovative Network solutions are necessary. Many of the aircraft, ships, tanks, and artillery systems of the joint force have been improved, in some cases exponentially, through the



incorporation of state-of-the-art C4 solutions. The Network requires corresponding investment and improvements, from home station to the deployed soldier, to fully enable these systems.

To realize the power of the Network, there are essential Network imperatives that must be achieved. Failure to do so will put in jeopardy the ability of the joint force commander and subordinate commanders to realize the full potential of operating in the information age. The three Network imperatives are availability, interoperability and control. These imperatives, outlined in Figure 4, support the tenets of strategic agility and operational flexibility and have application at all levels. Decisions on Network formations, investments, training, standards, tactics, techniques, and procedures (TTP) must be synchronized with these imperatives and lead to a pervasive global network.

**NETWORK AVAILABILITY** - Networks do not simply appear; they must be planned, resourced, maneuvered, and sustained. Network availability includes:

- Seamless, on demand access to enterprise and GIG services.
- Rapid expansion and self-healing.
- Connection of the Network to Army, joint, interagency, and coalition forces.
- Enterprise technical standards for all Network resources.
- Long range planning for infostructure expansion and upgrade.

**NETWORK INTEROPERABILITY** - Network interfaces and their enforcement are required to fight effectively in the joint battlespace. Network interoperability includes:

- Planning interaction with the Combatant Command Theater C4 Control Center (TCCC) and Theater NetOps Center (TNC).
- Interface to interagency, multinational, coalition, joint, and non-government organizations and commercial service providers.
- Joint standards and global configuration control for C4 systems and data services.

**NETWORK CONTROL** - Assured net-centric services across the Network support the full spectrum of warfighting, intelligence, and business missions. Network control includes:

- Centralized operation and management of the LandWarNet and access to GIG services.
- System installation and restoral.
- Security and defense.
- Collaborative information exchange.
- Control and allocation of critical resources (e.g., satellite bandwidth, spectrum, etc.).
- Situational awareness to assess impact on warfighter capabilities.

Figure 4

## CONCLUSIONS

The Network enables joint and expeditionary battle command through the use of joint procedures, systems, and connectivity and allows the commander to “see first, understand first, act first, and finish decisively.” The Network encompasses all aspects of the joint fight from maneuver to sustainment of the force. It must be a single integrated entity and not a collection of stovepipes. The Network must evolve to the point where deployment of extensive analytical, management, and support headquarters is no longer required. This Network transformation must embrace not just the battlefield but home station and sanctuary operations.

Network formations must provide scaleable, joint interoperable capabilities that are operated, defended, trained, equipped, and fought under global standards, protocols, processes, and configurations. This will require sustained, focused investment that follows a common, joint architecture and directly leads to like capabilities and equipment throughout all levels. Change to current governance processes and policies will be essential to achieve the necessary levels of centralized management and standardization. Force design must support the requirement for modular, scaleable, and secure capabilities at all echelons.

Although the joint force and Army fight by echelon, the pervasive nature and global interdependency of the Network, unbounded by space and time, requires that it be fought with a different paradigm, leveraging global operations and cyber defense capabilities at strategic and national levels. This paradigm requires a centrally managed enterprise that can reach instantaneously through all operational levels, the precise application of technology, and the attention of commanders at all echelons.

Without global unity of effort, the Network breaks. The Network must be fought by a Network commander at all levels, from the power projection platform to the UEy, UEx, and BCT. Commanders must have direct access to their supporting Network commander to enable unfettered interpretation of the commander’s intent for priorities, defense, restoration, sustainment, etc. Just as combat formations are maneuvered to have the maximum impact on the operations, so too must the Network assets be maneuvered to have the greatest impact. Network commanders must have unity of effort to successfully fight and defend the Network and deliver critical global C4 enablers to joint and expeditionary forces. Network commanders must be accountable for the entire network infrastructure and must manage all networks (battle command, intelligence, logistics, personnel, medical, etc.) at the respective echelon to enable warfighter needs.

This interdependent nature of the Network requires one (global) Network commander whose responsibilities extend beyond a single theater and include interface and synchronization with other Army, joint, and military service elements. This absolute requirement for network control requires unity of the Network across the enterprise, which necessitates a transformational approach to acquisition, modernization, and technology refreshment. The Army has already taken steps to enable Network transformation by creating an enterprise framework and global command relationships. These relationships, coupled with centralized management, technical control, and configuration management authorities, take on greater relevance and scope under

## Fight the Network

Army transformation. Acquisition, technology insertion, software standards, force modernization, life cycle replacements and upgrades, operational architectures, and TTPs must be centrally managed throughout the enterprise, down to the BCT level in order to realize the power of the Network.

There are additional requirements for the Network that must be enforced for the UEy. It is at the UEy that the fusion of battlefield operating systems occurs (with local, theater, and national assets) to support the ASCC. Therefore, the UEy must have a theater network command that is scaleable and tailored and fully integrates strategic and tactical Network formations under the UEy. The UEy commander must have direct access to and operational control over the UEy theater network commander to rapidly maneuver network forces. The UEy theater network commander must be responsible for the enterprise health and functionality of all echelons in the theater. To ensure fully integrated and synchronized planning and operations, the theater network commander must be dual hatted as the UEy G-6. This direct-access, dual-hatted relationship and Network responsibility will synchronize battle command, facilitate planning and execution of operational missions, and allow the prosecution of joint and combined operations.

This Fight the Network paradigm is complementary to the Joint NetOps CONOPS and has proven effective in current operations. For example, the CFLCC employed joint network and joint NetOps in OIF to enable his wartime headquarters to see the battle and employ his forces to great effect.

"...provided me an unprecedented ability to command and control my forces engaged in combat operations. I was able to 'see the battle' as it unfolded at incredible speed. The C4ISR networks they installed were responsive to the demands of a joint and coalition warfight, utilizing technologies and battlefield systems never before integrated, or even attempted, at the Operational Level." *LTG McKiernan, CFLCC Commander, Jun 03*

The Signal Regiment's challenge is to build upon this success and fully enable Army transformation. The Fight the Network paradigm presented in this white paper will enable the Signal Regiment to guide signal transformation and DOTML-PF development. Modern warfare is immensely complex and requires interoperability, synchronization, and synergy of all systems to achieve full spectrum dominance. Never before has the Signal Regiment been so critical to the success of our Army.